Tinjauan Pada Algoritma LFSR (*Linear Feedback Shift Register*) Dalam Reposisi XOR Dalam Pencarian Bilangan Acak Terbaik (Studi Kasus : LFSR Dengan 4 Bit dan 6 Bit)

[1]Angga Sulistiyanto , [2]Alz Danny Wowor
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50711, Indonesia
Telp : (0298) 321212, Fax : (0298) 321433
Email : [1)] 672015606@student.uksw.edu, [2)] alzdanny.wowor@staff.uksw.edu

Abstract

Cryptography or often called with science or art to maintain the confidentiality of an information. The linear feedback shift register (LFSR) algorithm is a generator that produces pseudo-bit numbers or shift register with linear feedback. This study looks for the best four-bit and six-bit random numbers using an exclusive OR (XOR) combination using the test runs test. Testing by entering four-bit binary and six bit binary numbers will be tested by exclusive OR (XOR) method, after which it will be shifted to right one bit, the first biyet is outputed after the shift result will be re-inserted for re-test. in XOR will be tested randomness with Runt test if test results less than 0.05 then the input test number is considered not random. The results produced nine random numbers that contained two numbers in the four-bit test and six were in the six-bit test

Keywords: Cryptography, LFSR, Run Test, exclusive OR (XOR)

Abstract

Kriptografi atau sering di sebut dengan ilmu atau seni untuk menjaga kerahasiaan sebuah informasi. Algoritma *linear feedback shift register* (LFSR) merupakan sebuah generator yang menghasilkan bilangan bit semu atau register geser dengan umpan balik linier. Penelitian ini mencari bilangan acak terbaik empat bit dan enam bit menggunakan kombinasi exclusive OR (XOR) dengan menggunakan pengujian Runs test. Pengujian dengan memasukkan bilangan biner empat bit dan enam bit akan di uji dengan metode exclusive OR (XOR),setelah itu akan di bangkitkan dengan metode LFSR (*linear feedback shift register)* geser ke kanan satu bit, biyet pertama dijadikan keluaran setela itu hasil antar pergeseran akan di masukkan kembali untuk di uji kembali.Setelah di XOR akan di uji keacakan dengan Runt test jika hasil pengujian kurang dari 0,05 maka masukan bilangan pengujian di anggap tidak acak. Hasil penelitian menghasilkan Sembilan bilangan acak yang terdapat dua bilangan di pegujian empat bit dan enam berada di pengujian enam bit.

Kata Kunci : K*riptografi, LFSR, Run Test, exclusive OR(XOR)*

[1)]Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana.
[2)]Staff Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana

UNIVERSITAS KRISTEN
SATYA WACANA
1956